



City of San Antonio

Information Technology Services Department

Policy #: 7-9000-S.004 v1.5

Information Security Technical Controls Policy

Planned Effective Date: May 14, 2010
Policy Owner: John Byers (207-2206)
Policy and Standards Manager: Alan Smith (207-0547)
Replaces and Supersedes: New

Document Status	Document Number	Published Date	Action Required	Due Date
First Draft	v. 1.3	04/12/10	Review/Provide Feedback	04/27/10
Second Draft	v. 1.4	05/04/10	Review/Provide Feedback	05/11/10
Final Version	v. 1.5	05/14/10		

TABLE OF CONTENTS

SECTION 1 POLICY SUMMARY..... 3

1.1 PURPOSE 3

1.2 GENERAL POLICY STATEMENT 3

SECTION 2 GENERAL GUIDELINES..... 4

2.1 TECHNICAL SECURITY 4

 2.1.1 *Identification* 4

 2.1.2 *Authentication* 4

 2.1.3 *Access Control Authorization* 4

 2.1.4 *Audit Trails* 5

2.2 SOFTWARE AND DATA SECURITY 5

 2.2.1 *General Software Security Elements* 5

 2.2.2 *Software Controls* 6

 2.2.3 *Software Security Implementation Procedures*..... 6

 2.2.4 *Data Controls*..... 6

 2.2.5 *Processing Environments*..... 6

2.3 NETWORK AND COMMUNICATION SECURITY 6

 2.3.1 *External Connections*..... 6

 2.3.2 *Notification* 7

 2.3.3 *Telecommuting/Remote Security*..... 7

APPENDIX A: INFORMATION SECURITY GLOSSARY 8

Section 1 Policy Summary

1.1 Purpose

The purpose of this policy is to protect City information assets through the implementation of technical controls, which provide automated protection against unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

1.2 General Policy Statement

All City information assets shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction – whether accidental or intentional – in order to maintain their confidentiality, integrity, and availability.

Pursuant to City Administrative Directive (AD) 7.8.1, *Information Security Program*, the City shall develop and implement technical controls for its information assets as they are defined in IT Policy 7-9000-S.001, *Information Security Asset Classification*. Technical controls are controls that computer systems execute. These technical controls shall include, but are not limited to:

- Technical Security
- Software and Data Security
- Network and Communications Security

Section 2 General Guidelines

2.1 Technical Security

2.1.1 Identification

Identification is the means by which a user provides a claimed identity to an information asset. The most common form of identification is a user ID.

- *Unique Identification.* Every City information asset must ensure that users are uniquely identified before being allowed to perform any action in the asset.
- *Correlate Actions to Users.* Each information asset must internally maintain the identity of all active users and be able to link actions to specific users.
- *Maintenance of User IDs:*
 - Departments shall ensure that all user IDs belong to currently authorized users.
 - Identification data shall be kept current by adding new users and deleting former users.
 - User IDs that are inactive for 90 days shall be disabled.

Assets designed to protect anonymity are, by their nature, exempt from requirements for User IDs.

2.1.2 Authentication

Authentication is the means of establishing the validity of a claimed identity to access an information asset. The City shall implement the following authentication controls:

- *Require Users to Authenticate.* Users shall authenticate their claimed identities on all information assets, as available.
- *Limit Log-on Attempts.* Per AD 7.6 – *Security and Passwords*, the City shall limit the number of log-on attempts to three (3).
- *Administer Data Properly.* The City shall have procedures to disable lost or stolen passwords and shall monitor systems to look for stolen or shared accounts.
- *Passwords.* Per AD 7.6 – *Security and Passwords*, the City shall implement controls to require strong passwords.

2.1.3 Access Control Authorization

Access is the ability to perform a function (e.g., use, change, or view) with an information asset. Access controls are the means by which the ability is explicitly enabled or restricted in some

way. Access controls can prescribe not only who (a user) or what (a process) is to have access to a specific system resource, but also the level of access that is permitted.

Per *AD 7.8D – Account Access Management* and *7.8E – User Account Management*, information asset owners shall establish a process to authorize and document access privileges based on a legitimate and demonstrated need to have system access. Access privilege documentation shall be maintained in a manner that makes it easily retrievable by individual user account. Any default “Guest” account shall be disabled.

The City shall control access to resources based on the following access criteria, as appropriate:

- *Identity.* The identity shall be unique (e.g., User ID) in order to support individual accountability.
- *Roles.* Access to information shall be controlled by the job assignment or function (i.e., the role) of the user who is seeking access.
- *Affiliation.* Access to particular system resources shall be based upon organizational assignment or association.

2.1.4 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. Audit trails provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. The City shall protect an audit trail from unauthorized access by individuals without the need to know. ITSD, in collaboration with the City Auditor, City Clerk, and business owner of the information asset, shall determine the appropriate retention schedule for audit trails.

An audit trail must include sufficient information to establish what event occurred and who (or what) caused them. The scope and contents of the audit trail will balance security needs with performance needs, privacy, and costs. At a minimum, the audit trail must specify:

- Type of event
- When the event occurred (time and day)
- User ID associated with the event
- Program or command used to initiate the event

2.2 Software and Data Security

2.2.1 General Software Security Elements

Per *IT Policy 7-9000-S.005 – Information Asset Certification and Accreditation Policy*, all information assets shall be accredited prior to use. Information assets shall be obtained through authorized procurement channels.

2.2.2 Software Controls

Design reviews shall be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements required by the information asset's classification and risk level.

New or substantially modified confidential assets, such as software, must be thoroughly tested prior to implementation to verify that the required security controls are present and are operationally adequate. This is usually accomplished as part of the certification and accreditation (C&A) process.

2.2.3 Software Security Implementation Procedures

All security related software updates, security patches, and similar security improvements shall be promptly tested, installed, and documented for all City information assets, as they become available.

2.2.4 Data Controls

Departments shall use encryption to protect confidential data in transit and at rest. Departments shall work with ITSD to obtain the required software and/or hardware.

Effective October 1, 2010, all newly acquired information assets shall provide for encrypted data storage, as necessary.

Effective January 15, 2011, all portable devices shall encrypt the data stored on the device. All laptops, notebooks, tablet PCs, and other portable devices shall utilize full-disk encryption (FDE). This includes, but is not limited to, all portable data storage devices such as personal digital assistants (PDA), flash drives, compact disks (CD), digital video disks (DVD), iPhones, Blackberries, Smart-Phones, or any other external, remote, and portable storage devices.

Effective November 01, 2012, all City information assets, as necessary, shall encrypt all data processed using Federal Information Processing Standards (FIPS) encryption standards. FIPS are publicly announced standards developed by the US Federal government for use by all non-military government agencies and by government contractors.

2.2.5 Processing Environments

City automated information assets use several processing environments that meet the specific and varied needs of users. The production environment is the environment for the processing of official data utilized in support of business missions and management. The production environment shall adhere to all Federal, State, and municipal regulations, policies, and guidelines. The development, testing, training, and other similar environments are for the purposes of maintenance, modification, and enhancement. Data in these environments must adhere to the security controls required based upon their classification.

2.3 Network and Communication Security

2.3.1 External Connections

An external connection is any connection from an outside network (a source other than the City) that is electronically linked to a system or network that is owned or operated by or in behalf of the City. External connections must adhere to the directives established in *AD 7.8C – Remote Access*.

2.3.2 Notification

ITSD shall establish a notification system for threats and security risks for users, business owners, and system administrators of information assets, as appropriate.

2.3.3 Telecommuting/Remote Security

The security of City assets at an alternative work site (e.g., home, hotel) is just as important as it is at a City facility. Per *AD 7.5 – Acceptable Use of Information Technology*, reasonable precautions must be taken at alternative work sites to protect City information assets from theft, damage, and misuse. Users shall not discard confidential information at home, in hotel wastebaskets, or other publicly accessible trash containers. Per *AD 7.8C – Remote Access*, users who are remotely connected to City networks shall maintain security controls commensurate with the information asset they are accessing.

Appendix A: Information Security Glossary

<i>Access Control</i>	Security control designed to permit authorized access to an IT system or application.
<i>Accreditation</i>	Authorization by the Information Technology Services Department (ITSD) Chief Technology Officer (CTO), or designee, to place an IT system into operation.
<i>Audit Trail</i>	A record showing who has accessed a computer system, when, and what operations he or she has performed during a given period. Audit trails are useful both for maintaining security and for recovering lost transactions.
<i>Authentication</i>	The process of determining whether someone or something is, in fact, who or what it is declared to be.
<i>Availability</i>	Ensuring that information systems, including stored information and processing capability, are always available to authorized users when needed.
<i>Backup</i>	A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.
<i>Certification</i>	The technical and non-technical evaluation of an IT system – by the system owner or by an independent certifying agent – that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place an IT system into operation.
<i>Ciphertext</i>	Form of cryptography in which the plaintext is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.
<i>Classification</i>	A systematic arrangement of objects into groups or categories according to a set of established criteria.
<i>Commercial-Off-The-Shelf (COTS) Software</i>	Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

<i>Confidentiality</i>	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
<i>Configuration Management</i>	The process of keeping track of changes to the system, if needed, approving them.
<i>Contingency Plan</i>	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.
<i>Controls</i>	The means of managing risk, which includes policies, procedures, guidelines, practices, or organizational structures. Controls may be management (e.g., risk management plan), operational (e.g., strong password rules), or technical (e.g., corporate firewalls) in nature.
<i>Corrective Actions</i>	Steps that are taken to address existing nonconformities and make improvements. Corrective actions deal with actual nonconformities (problems), ones that have already occurred. They solve existing problems by removing their causes. In general, the corrective action process can be thought of as a problem solving process.
<i>Data</i>	Information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's CPU and stored in files and folders on the computer's hard disk.
<i>Degaussing Media</i>	Method to erase data from magnetic tape magnetically.
<i>Document</i>	A form of information. A document can be put into an electronic form and stored in a computer as one or more files. Often a single document becomes a single file. An entire document or individual parts may be treated as individual data items. As files or data, a document may be part of a database.
<i>File</i>	A collection of data stored in one unit, identified by a filename. It can be a document, picture, audio, or video stream, data library, application, or other collection of data.
<i>Friendly Termination</i>	The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.
<i>Gateway</i>	A bridge between two networks.

<i>Hardware</i>	Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.
<i>Information Asset</i>	All records, documents, data, and systems created, owned, or managed by the City.
<i>Information Asset Owner</i>	A person or group of people with authority and responsibility for establishing the controls for an information asset's generation, collection, processing, dissemination, and disposal.
<i>Information Security</i>	Measures taken to preserve the confidentiality, integrity and availability of information; ensures that information is authentic, reliable, and from an accountable source.
<i>Information Security Plan</i>	Document that details the security controls established and planned for a particular system.
<i>Information System</i>	Computers, hardware, software, storage media, and networks; the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
<i>Information System Administrator</i>	The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.
<i>Information System Owner</i>	The individual who is ultimately responsible for the function and security of the system.
<i>Integrity</i>	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
<i>Intrusion Detection</i>	Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
<i>Issue-Specific Policy</i>	Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

<i>IT Security</i>	Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of IT systems and data. IT security includes consideration of all hardware and/or software functions.
<i>IT Security Policy</i>	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
<i>Least Privilege</i>	The process of granting users only those accesses they need to perform their official duties.
<i>Local Area Network</i>	A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.
<i>Management Controls</i>	Security methods that focus on the management of the computer security system and the management of risk for a system.
<i>Network</i>	Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.
<i>Operating System</i>	The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.
<i>Password</i>	Protected/private character string used to authenticate an identity or to authorize access to data.
<i>Port</i>	An interface on a computer to which you can connect a device.
<i>Port Protection Device</i>	A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

<i>Preventive Actions</i>	Steps that are taken to avoid potential nonconformities and make improvements. Preventive actions address potential nonconformities (problems), ones that have not yet occurred. Preventive actions prevent the occurrence of problems by removing their causes or reduce the likelihood that they will occur. In general, the preventive action process can be thought of as a risk management process.
<i>Private Branch Exchange (PBX)</i>	A private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.
<i>Record</i>	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Record definitions for the City of San Antonio are contained in COSA Administrative Directive 1.34.
<i>Remote Access</i>	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information
<i>Risk</i>	The possibility that an event that will adversely impact the City's information assets. The potential risk is measured by the cost of the risk to the City, if realized, discounted by the probability, or the likelihood, that the risk will occur.
<i>Risk Assessment</i>	A process to identify, analyze, and manage potential risks.
<i>Risk Management</i>	Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.
<i>Sensitive Information</i>	Any information, the loss or misuse of which could adversely affect the privacy to which individuals are entitled.
<i>Sensitivity</i>	A measure of the importance assigned to information by its owner, for denoting its need for protection.
<i>Software</i>	Computer instructions or data. Anything that can be stored electronically is software.
<i>Technical Security Policy</i>	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

<i>Telecommunications</i>	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.
<i>Threat</i>	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.
<i>Trojan Horse</i>	Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.
<i>User</i>	Any person who is granted access privileges to a given IT.
<i>Virus</i>	A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.
<i>Vulnerability</i>	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.